

نريد لدينا عدد صحيح 962

(1) اكتبه في باقي قسمة 4 (0) أو (1)

$$a^2 \equiv 0 \text{ or } 1 \pmod{4}$$

(2) إذا كان  $n$  عدد طبيعي أكبر من (1) يتوي في العدد

جميع مراتبه العشرية فلا يمكن أن يكون مربعاً كاملاً

(أما لا يمكن إيجاد عدد صحيح مربع هو ذلك العدد (11111111))

الحل عند تقسيم  $a$  على 4 فحصل على إحدى الحالات التالية:

$$a = 4q \Rightarrow a^2 = 16q^2 = 4(4q^2) \quad k$$

$$a = 4q + 1 \Rightarrow a^2 = 16q^2 + 8q + 1 = 4(4q^2 + 2q) + 1 \quad k \in \mathbb{Z}$$

$$= 4k + 1$$

$$a = 4q + 2 \Rightarrow a^2 = 16q^2 + 16q + 4 = 4(4q^2 + 4q + 1) \quad k$$

$$= 4k + 1$$

$$a = 4q + 3 \Rightarrow a^2 = 16q^2 + 24q + 9 = 16q^2 + 24q + 8 + 1$$

$$= 4(4q^2 + 8q + 2) + 1 = 4k + 1$$

2.  $n$  عدد طبيعي أكبر من الواحد ( $n > 1$ ) جميع مراتبه واحد

$$n = 111 \dots 111$$

$$= 111 \dots 100 + 11$$

$$n = 4q + 8 + 3$$

$$= 4(q + 2) + 3 = 4k + 3 \quad k = q + 2 \in \mathbb{Z}$$

$$n = 4k + 3$$

باقي قسمة  $n$  على (4) هو (3) أي لا يساوي (0) أو (1)ومن ثم  $n$  ليس مربعاً كاملاً، لأن لا يمكن إيجاد عدد صحيح مربعهيساوي  $n$ 

الفصل الأول انتهى



## القواسم المشتركة

القواسم المشتركة والحد الأدنى المشترك

تدريج نقول ان العدد الصحيح  $d \neq 0$   $\mathbb{Z} \ni d$  انه قاسم مشترك للعددين الصحيحين  $a$  و  $b$   $\mathbb{Z} \ni d$  غير الصفرين اذا كان  $d | a$   $\wedge$   $d | b$

ملاحظات:

1. اذا كان  $(d, a)$   $\wedge$   $(d, b)$  فبان  $(d, a)$   $\wedge$   $(d, b)$

2. ان القاسم المشترك  $d$  بالقيمة المطلقة لا يتجاوز العددين  $a$  و  $b$  بين العددين  $|d| \leq |a|$  و  $|d| \leq |b|$  و  $a \cdot b \neq 0$

$$|d| \leq |a|$$

$$|d| \leq |b|$$

3. ان مجموعة القواسم المشتركة الموجبة لعددين صحيحين غير صفرين هما تقاطع مجموعتي القواسم الموجبة لـ  $a$  مع مجموعة القواسم الموجبة لـ  $b$  فهي حقا مجموعة منتهية.

تعريف: القاسم المشترك الأعظم:

نقول ان العدد  $d$  هو القاسم المشترك الأعظم للعددين  $a$  و  $b$  غير الصفرين

$$g.c.d.(a, b) = d = d(a, b) = (a, b)$$

اذا كان

$$d > 0$$

$$d | a \wedge d | b$$

اذا وجد قاسم آخر  $a$  و  $b$  مثل  $c > 0$  بحيث  $c | a$  و  $c | b$

$$c \leq d$$

ملاحظة: هنا ومن الملاحظة (\*) ان القاسم المشترك الأعظم لعددين غير صفرين

موجود دائما ووحيد

ملاحظة: اذا كان  $a = b = 0$  فبان مجموعة القواسم المشتركة هي كل  $\mathbb{Z}$

فهي مجموعة غير منتهية وليس بينها عنصر أكبر من ثم لا يوجد قاسم

مشترك أعظم



**مبرهنة** إذا كان  $a, b$  عددين صحيحين غير معددين فإن القاسم المشترك الأعظم لهما هو تركيب خطي لهذا العددين.

أي يوجد دائماً عدداً صحيحين  $x, y \in \mathbb{Z}$  :  $d(a, b) = d = ax + by$ .

$$\text{مثال: } d(12, 15) = 3$$

$$3 = 1 \cdot 12 + (-1) \cdot 15$$

$$3 = 1 \cdot 12 + (-1) \cdot 15$$



**ملاحظة:** إن القاسم المشترك الأعظم لعددين غير معددين هو العنصر الأصغر لمجموعة التراكيب الخطية الموجبة للعددين  $a$  و  $b$ .

**نتيجة:** إذا كان  $c$  قاسم لـ  $a$  و  $b$  فهو حتماً قاسم لـ  $d(a, b)$ .

**مبرهنة** إذا كان القاسم المشترك الأعظم لعددين صحيحين يساوي (1) فإننا نسمي هذين العددين أوليين نسبياً فيما بينهما.

**مبرهنة في هذه الحالة التي:**

يكون العددا  $a$  و  $b$  غير المعددين أوليين نسبياً فيما بينهما إذا وفقط إذا  $ax + by = 1$  عدداً صحيحين  $x$  و  $y$  بحيث أن

**إدبات:**

$\Rightarrow$  نفرض أن  $a, b$  أوليان فيما بينهما  $d = (d(a, b) = 1)$

ومسبب برهنة سابقة، يوجد عدداً صحيحين  $x_0, y_0$  و  $ax_0 + by_0 = 1$

$$ax_0 + by_0 = 1$$

$\Rightarrow$  نفرض الآن وجود عدداً صحيحين  $x$  و  $y$  بحيث أن

$$ax + by = 1 \quad x, y \in \mathbb{Z}$$

ولكن  $d = d(a, b)$  أي  $d \mid a$  و  $d \mid b$   $\Rightarrow d \mid (ax + by) = 1$

$$d \mid (ax + by) = 1 \Rightarrow d = 1$$

أي أن العددين  $a$  و  $b$  أوليان نسبياً فيما بينهما.

نتج من هذا ما شئنا.



$$d = d(a, b)$$

بمقتضى إذا كانت

$$\Rightarrow d\left(\frac{a}{b}, \frac{b}{d}\right) = 1$$

نريد اثبات أن القاسم المشترك لـ  $a, b$ 

$$d(a, b) = d(a, b - ac)$$

بعض خواص القاسم المشترك

$$1) d(-a, -b) = d(a, b) \Rightarrow d(a, -b) = d(-a, b) \\ = d(|a|, |b|) = d(a, b)$$

$$2) d(1, a) = 1 \\ d(0, a) = |a|$$

$$3) d(a, m) = d(b, m) = 1 \\ \Rightarrow d(a \cdot b, m) = 1$$

القاسم المشترك لأعداد صحيحة  $a, b$   
 حيث  $a, b$  أولي مع  $m$

$$4) d(k, b) = 1 \wedge k | (a, b) \\ \Rightarrow k | a$$

$k$  يقسم  $a, b$  العددين  $a, b$   
 وإذا كانت  $k$  عدد أولي ويقسم  $a, b$  العددين  
 فإن  $k$  يقسم  $a$  أو  $b$

إذا كانت  $p$  عدد أولي ويقسم  $a, b$  عددين  $a, b$  فإنه يقسم أحدهما

$$p | a \cdot b \Rightarrow p | a \text{ or } p | b$$

$$4 | 12 = 3 \cdot 1$$

$$d(4, 3) = 1$$

$$4 | 12 = 2 \cdot 6$$

$$4 | 6$$

شرط استحقاق أن يكون  $k$  أولي مع  $a, b$  العددين

$$d = d(a, b) \Rightarrow d(ma, mb) = m \cdot d$$

أثبت ذلك  
 صراحة



## خوارزمية إقليدس:

نصيب  $a, b$  إذا كان  $0 < r < a$  عدد صحيحوكان  $0 < r < a$  و  $b = qa + r$  فبا  $c$ 

$$d(b, a) = d(a, r)$$

$$d(a, b) = d \Rightarrow d|a \wedge d|b$$

$$\Rightarrow d|(b + (-q)a) = r$$

نلاحظ  
كلتا  $a$  و  $b$  مشتركة لـ  $d$   
وكلتا  $a$  و  $r$  مشتركة لـ  $d$ 

كل قاسم مشترك لـ  $a, b$  يجب ان يقسم  $r$  اي ان  $d$  يقسم  $r$   
لناخذ  $c$  عددا بحيث ان  $c$  قاسم لـ  $a, r$  فلهذا قاسم لـ  $qa + r$   
اي  $c$  قاسم لـ  $b$

وبهذا ان  $c$  قاسم لـ  $a$  بالضرورة  $c|d$   
اي ان القاسم المشترك الاكبر لـ  $a, r$  هو نفسه  $d$

## خوارزمية إقليدس:

في وسيلة لإيجاد القاسم المشترك الأعظم لعددين معينين وكنا بته ايضا  
كتركيب قطري لهما، ويتم ذلك وفق عمليات قسمة متتالية  
وصية ١  $d(a, b) = d(a, a \bmod b)$  فيمكن ان نعتبر عددا ان  
العددين موجبات تماما

ان البحث عن القاسم المشترك الأعظم لعددين موجبين يتطلب خوارزمية القسمة  
بشكل متتال حتى نصل الى ابوابي الصغرى ويكون عندئذ ابوابي ارقير قبل ابوابي  
الصغرى هو القاسم المشترك الأعظم الذي نبحث عنه.

والمثال الذي سوف نذكره

العدد القاسم المشترك الأعظم للعددين  $30$  و  $72$  كتركيب قطري لهما

$$72 = 2 \cdot 36 + 0$$

نقسم على الباقي  
القاسم المشترك الأعظم لهما

$$30 = 2 \cdot 12 + 6$$

$$12 = 2 \cdot 6 + 0$$

$$6 = 30 - 2 \cdot 12 = 30 - 2(72 - 2 \cdot 36)$$

$$6 = 5(30) + (-2)72$$

٣٠

٧٢







$$\text{lcm}(a, b) = L(a, b) = (a, b)$$

## المضاعف المشترك الأصغر

تعريف: لنكن  $a, b$  أعداد صحيحة غير صفرية ( $a, b \neq 0$ )

نقول أن العدد  $m$  مضاعف مشترك لهذه الأعداد إذا كانت مضاعفاً لكل منهما.

$$\forall a \mid m, \forall b \mid m \quad (a, b \neq 0)$$

ونقول أن العدد  $L$  هو المضاعف المشترك الأصغر لهذه الأعداد  $a, b$  ( $a, b \neq 0$ ) إذا كانت:

$$L > 0$$

$$\forall a \mid L, \forall b \mid L \quad (a, b \neq 0)$$

$$(3) \text{ إذا كانت } m < L \text{ حيث } m \mid a, m \mid b \text{ لكل } (a, b \neq 0)$$

$$L \leq m$$

نتج ما نعرفه هنا أن المضاعف المشترك الأصغر هو أصغر المضاعفات المشتركة. وأن المضاعف المشترك الأصغر يقسم أي مضاعف آخر لهذه الأعداد. ويرسم الشكل.

$$\left. \begin{array}{l} d(a, b) = d \\ L(a, b) = L \end{array} \right\} \Rightarrow \begin{array}{l} \text{إذا كانت } a, b \text{ عددين صحيحين موجبين وكانت} \\ d \cdot L = a \cdot b \\ L(a, b) = \frac{a \cdot b}{d(a, b)} \end{array}$$

أي:

أي:

انظر المثال  
عدد 45 كتابت  
بشكل

$$g \mid d(a, b) \cdot \text{lcm}(a, b) = (a, b)$$

$$\text{نتيجة: إذا كانت } a, b \text{ عددين صحيحين موجبين} \\ d(a, b) = 1 \quad \text{فإن} \quad \text{lcm} = a \cdot b$$

الفصل الثاني: التقدير



الأعداد الأولية وبعض خواصها.

نقول ان العدد  $p$  اولي اذا كان  $p > 1$  وكان لا يقبل القسمة إلا بنفسه أو 1 (لا  $p$  يملك قاسمًا مشتركًا مختلفين فقط  $(1, p)$  وفيما عدا ذلك يدعى عدداً مؤلفاً (مركباً)).  
 ويسمى العدد الصحيح الموجب غير الأولي  $n$  كبرن (1) بأنه عدد مؤلف.

$$n = a \cdot b \quad 1 < a < n \quad 1 < b < n$$

بعض الخواص الأساسية:

1- ان  $n$  عدد اولي  $p$  اعداد اولية نسبياً متى شئت.  $(2, 3, 5, 7)$

2- اذا كان  $p$  يقسم  $n$   $(p|n)$  فإن  $d(p, n) = p$

فإذا لم يقسم  $(p \nmid n)$  فإن  $d(p, n) = 1$

3- اذا كان  $p$  عدد اولي وقسم جداد عددين صحيحين فهو يقسم أحدهما. يقسم أحد العددين

$$p|a \cdot b \iff p|a \text{ or } p|b$$

$p|a_1 \cdot a_2 \cdot \dots \cdot a_n \iff p|a_i$  فإن  $p$  يقسم أحد المضارب مع الأقل

نقطة: اذا كانت  $a_1, a_2, \dots, a_n$  وكانت  $a_i$  أعداد أولية

فإن العدد الأولي  $p$  يساوي أحد المضارب مع الأقل (إذا كانت أولية).

المبرهنه الأساسية في الحساب:

أي عدد صحيح  $n \in \mathbb{Z}$  هو إما عدد اولي أو أنه جداد عدد منتهى من الأعداد الأولية، وهذا التمثيل كجداد عوامل أولية يكون وحيداً (بإهمال ترتيب الضاربين).

$$12 = 2^2 \cdot 3$$

برهان: يمكن أن تكون بعض العوامل الأولية لعدد صحيح متساوية، نأخذ بعضاً بعضاً العوامل

المتساوية، يمكننا كتابة العدد  $n$  كجداد عوامل أولية  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$  بالتركيب،

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k} \quad \text{حيث } p_1 < p_2 < \dots < p_k \text{ أعداد أولية.}$$

نقطة: كل عدد صحيح  $n$   $n > 1$  له عامل أولي



$$n = a \cdot b; \quad 1 < a \leq b < n$$

$$n = a \cdot b \geq a^2$$

$$\sqrt{n} \geq a$$

کتاب

$$p \mid n = a \cdot b$$

$\rho \in \rho_{1A}$

۲)  $p$  قسم  $a$  نهو اهنر اويي ساري  $a$   $p \leq a$

$p \leq \sqrt{n} \iff a \leq \sqrt{n}$  ولذا

$$\rho \leq \sqrt{n}$$

فَحَمًّا يَكُونُ دَعْدًا أَوَّلِيًّا

عمر سے پہلے میں ان کا ان العدد (731) عدداً مدلفاً احم عدداً اولیاً

دوره: تکریمه اجبت آن  $m$  عدد آوی تقسیم  $p < z < 1$  و  $Pl\left(\frac{p}{z}\right)$   
 اخله ناقه  $\left(\frac{p}{z}\right)$

$$\binom{p}{j} = \frac{p!}{j!(p-j)!} = \frac{p(p-1) \cdots (p-j+1)(p-j)!}{j!(p-j)!}$$

$$= \frac{p(p-1) \cdots (p-j+1)}{j!}$$

نقل إلى الفرق الثاني

$$j! \binom{p}{j} = p(p-1) \dots (p-j+1)$$

مقيم الطرف الايمن بالتاكيد

$$P \text{ 15! } \left( \begin{matrix} P \\ j \end{matrix} \right)$$

م اوی وسم جداد مزدرب زهد بسم اعد المقدرب

لوکی ج 3.2.1 - (1-2)  $Pl$  و  $PC$  ماری فسیقہ امد المضاربت

وکی صیغہ مضاریب  $\uparrow$  اعلیٰ سے  $P$  فرضاً: اِذَا  $P$  از  $P$

$$P_1\left(\frac{P}{2}\right)$$